2024-1492, 2024-1493

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

CPC PATENT TECHNOLOGIES PTY LTD.,

Appellant,

v.

ASSA ABLOY AB, ASSA ABLOY INC., HID GLOBAL CORP., ASSA ABLOY GLOBAL SOLUTIONS, INC., MASTER LOCK COMPANY, LLC,

Appellees.

Appeals from the United States Patent and Trademark Office, Patent Trial and Appeal Board in Nos. IPR2022-01093, IPR2022-01094.

RESPONSE BRIEF OF APPELLEES ASSA ABLOY AB, ASSA ABLOY INC., HID GLOBAL CORP., ASSA ABLOY GLOBAL SOLUTIONS, INC., MASTER LOCK COMPANY, LLC

Lionel M. Lavenue
Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
1875 Explorer Street, 8th Floor
Reston, VA 20190-6023
(571) 203-2700

Attorneys for Appellees ASSA ABLOY AB, ASSA ABLOY Inc., HID Global Corp., ASSA ABLOY Global Solutions, Inc., and Master Lock Company, LLC

Kara A. Specht
Benjamin Saidman
Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
271 17th Street, NW, Ste. 1400
Atlanta, GA 30363-6209
(404) 653-6400

Jonathan J. Fagan
Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
901 New York Avenue, NW
Washington, DC 20001-4413
(202) 408-4000

August 7, 2024

EXEMPLARY CLAIMS OF U.S. PATENT NO. 8,620,039

1. A method of enrolling in a biometric card pointer system,

the method comprising the steps of:

receiving card information;

receiving the biometric signature;

defining, dependent upon the received card information, a memory location in a local memory external to the card;

determining if the defined memory location is unoccupied; and

storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

Appx278 at 12:29-38 (emphasis added).

3. A method of securing a process at a verification station, the method comprising the steps of:

(a) providing card information from a card device to a card reader in the verification station;

(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

(c) determining if the provided card information has been previously provided to the verification station;

(d) if the provided card information has not been previously provided to the verification station;

(da) storing the inputted biometric signature in a memory at ***a memory location defined by the provided card information***; and

(db) performing the process dependent upon the received card information;

(e) if the provided card information has been previously provided to the verification station;

(ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

Appx278-279 at 12:51-13:11 (emphasis added).

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

CERTIFICATE OF INTEREST

Case Number: 2024-1492, 2024-1493

Short Case Caption: CPC Patent Technologies Pty Ltd. v. Assa Abloy AB

Filing Party/Entity: ASSA ABLOY AB, ASSA ABLOY Inc., HID Global Corp., ASSA ABLOY Global Solutions, Inc., Master Lock Company, LLC

Instructions:

1. Complete each section of the form and select none or N/A if appropriate.
2. Please enter only one item per box; attach additional pages as needed, and check the box to indicate such pages are attached.
3. In answering Sections 2 and 3, be specific as to which represented entities the answers apply; lack of specificity may result in non-compliance.
4. Please do not duplicate entries within Section 5.
5. Counsel must file an amended Certificate of Interest within seven days after any information on this form changes. Fed. Cir. R. 47.4(c).

I certify the following information and any attached sheets are accurate and complete to the best of my knowledge.

Date: August 7, 2024

Signature: /s/ Lionel M. Lavenue

Name: Lionel M. Lavenue

1. Represented Entities. Fed. Cir. R. 47.4(a)(1).	**2. Real Party in Interest.** Fed. Cir. R. 47.4(a)(2).	**3. Parent Corporations and Stockholders.** Fed. Cir. R. 47.4(a)(3).
Provide the full names of all entities represented by undersigned counsel in this case.	Provide the full names of all real parties in interest for the entities. Do not list the real parties if they are the same as the entities. ☐ None/Not Applicable	Provide the full names of all parent corporations for the entities and all publicly held companies that own 10% or more stock in the entities. ☐ None/Not Applicable
ASSA ABLOY AB	None	ASSA ABLOY AB
ASSA ABLOY Inc.	None	ASSA ABLOY AB
HID Global Corporation	None	ASSA ABLOY AB; ASSA ABLOY Inc.
ASSA ABLOY Global Solutions, Inc.	None	ASSA ABLOY AB; ASSA ABLOY Inc.
Master Lock Company, LLC	ASSA ABLOY Residential Group, Inc.	Fortune Brands Outdoors & Security, LLC; Fortune Brands Innovations, Inc.

☐ Additional pages attached

4. Legal Representatives. List all law firms, partners, and associates that (a) appeared for the entities in the originating court or agency or (b) are expected to appear in this **court** for the entities. Do not include those who have already entered an appearance in this court. Fed. Cir. R. 47.4(a)(4).

☐ None/Not Applicable ☐ Additional pages attached

Dion Bregman Morgan, Lewis & Bockius LLP		
Andrew Devkar Morgan, Lewis & Bockius LLP		
James Kristas Morgan, Lewis & Bockius LLP		

5. Related Cases. Other than the originating case(s) for this case, are there related or prior cases that meet the criteria under Fed. Cir. R. 47.5(a)?

☒ Yes (file separate notice; see below) ☐ No ☐ N/A (amicus/movant)

If yes, concurrently file a separate Notice of Related Case Information that complies with Fed. Cir. R. 47.5(b). **Please do not duplicate information.** This separate Notice must only be filed with the first Certificate of Interest or, subsequently, if information changes during the pendency of the appeal. Fed. Cir. R. 47.5(b).

6. Organizational Victims and Bankruptcy Cases. Provide any information required under Fed. R. App. P. 26.1(b) (organizational victims in criminal cases) and 26.1(c) (bankruptcy case debtors and trustees). Fed. Cir. R. 47.4(a)(6).

☒ None/Not Applicable ☐ Additional pages attached

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Rules

Regulations

STATEMENT OF RELATED CASES

Counsel for Appellees certifies that no other appeal from the same proceeding in the United States Patent and Trademark Office, Patent Trial and Appeal Board, is or was previously before this Court or another appellate court, whether under the same or similar title.

The Court's decision in this appeal can affect or be affected by the following cases:

- *ASSA ABLOY AB, et al. v. CPC Patent Technologies Pty. Ltd., et al.*, No. 3:22-cv-00694-MPS (D. Conn.);
- *CPC Patent Technologies Pty. Ltd. v. HID Global Corporation*, No. 6:22-cv-01170-ADA (W.D. Tex.); and
- *CPC Patent Technologies Pty Ltd. v. Apple Inc.*, No. 3:22-cv-02553-RFL (N.D. Cal.).

Further, this Court designated *CPC Patent Technologies Pty Ltd. v. Apple Inc.*, Appeal No. 24-1365 (an appeal from *Apple Inc. v. CPC Patent Technologies PTY, LTD.*, IPR2022-00600 (PTAB)), as a companion case.

I. PRELIMINARY STATEMENT

U.S. Patent No. 8,620,039 ("the '039 patent") is directed to security issues associated with the use of cards "such as credit cards, smart cards, and wireless card-equivalents such as wireless transmitting fobs." Appx273 at 1:13-16. These cards can be used for various purposes, including "drawing cash from an Automatic Teller Machine (ATM)," "making a purchase on credit," or accessing a secure building door. Appx273 at 1:25-29; Appx278 at 11:44-53. Each card contains "card information" that can be accessed "by 'coupling' the card device to an associated reader device." Appx273 at 1:23-25. To prevent fraud, card readers may use a verification system, such as requiring that a user presenting a card also provide a biometric signature (e.g., a scanned fingerprint). Appx273 at 1:33-2:44. This verification system compares the newly scanned fingerprint with a stored fingerprint image associated with an authorized user to verify user access. Appx276 at 8:34-41.

According to the '039 patent, conventional verification systems were cumbersome and slow because they required searching an entire database of biometric signatures to confirm that a given user's biometric signature was a match. *See* Appx276 at 8:34-41. CPC contends that the '039 patent solved this problem by using card information (e.g., an account number) to define a memory location in a local database at which a user's biometric signature will be stored. Blue Br. 1-2. Then, once a user enters a biometric signature, "the system only needs to check a

single memory address (*i.e.*, the specific address 'defined' by the 'card information')"—rather than search an entire database—to confirm that the biometric signature matches the stored data and "verify [that] user." *Id.* The '039 patent allegedly claimed this concept by reciting, in part, the steps of "defining, dependent upon the received card information, a memory location in a local memory external to the card" (the "Defining Limitation") and "storing, if the memory location is unoccupied, the biometric signature at the defined memory location." *E.g.*, Appx278 at 12:29-38 (claim 1).

But the prior art taught the methods and systems claimed by the '039 patent, including the Defining Limitation. The prior art Hsu reference (Appx943-950) discloses using card information and a biometric signature to verify a user's identity and "control[] access to building doors or to machines, such as automatic teller machines (ATMs)." Appx943, Abstract; Appx944 ¶¶ 1, 6; Appx993 ¶¶ 32, 33. Like the '039 patent, Hsu recognized that conventional biometric verification systems "have been relatively slow" because the "fingerprint matching system . . . must compare a sensed fingerprint image with many possible stored reference images" before verifying a card user. Appx944 ¶ 4. Hsu thus discloses storing a reference fingerprint image in a memory location "associated with" a user's card information so that only the user's card information is necessary to find the reference fingerprint. Appx945-946 ¶¶ 13, 20. Doing so allows "fingerprint matching" to "be achieved

rapidly," eliminating the need to "compare a sensed fingerprint with many possible stored reference images." Appx944-945 ¶¶ 13, 4.

A subset of Appellees[1] ("Petitioners") filed two petitions for *inter partes* review, collectively challenging claims 1-20 of the '039 patent. In the Final Written Decisions, the Board adopted CPC's construction of the Defining Limitation, construing the term to mean that "during an enrollment process[,] the claimed 'biometric signature,' e.g., a fingerprint, is not yet stored in the memory, and no memory location or address has been 'defined,' as in 'set' or 'established,' in the memory for storing the fingerprint, until card information is received."[2] Appx16.

The Board found that, under CPC's construction, Hsu disclosed the Defining Limitation by disclosing that a biometric signature is stored in a location "associated with" a user's card information. Appx33-34. The Board first found that "Hsu tells us a location, that is[,] *where*, i.e., in fingerprint database 44, the fingerprint is to be stored during enrollment." Appx33. According to the Board, the user's fingerprint is stored in relation to, i.e., "associated with," the user's card information. Appx33

---

[1] Appellee Master Lock Company, LLC, was not a petitioner before the Board. *See* Dkt. 23.

[2] The Board's Final Written Decisions in IPR2022-01093 and IPR2022-01094 are identical in relevant parts. Appx1-58; Appx59-125. For simplicity, citations to the Final Written Decisions will be only to IPR2022-01093 unless there is value in citing both.

(quoting Appx946-947 ¶ 26); Appx91 (quoting Appx946-947 ¶ 26). The Board also found that Hsu discloses how the fingerprint data is stored during enrollment. Appx33. In its Final Written Decisions, the Board found all challenged claims of the '039 patent unpatentable as obvious over the prior art. Appx2; Appx56-57; Appx60; Appx122-124.

CPC's sole argument regarding the prior art across both proceedings is the same factual dispute it now raises on appeal—whether Hsu discloses the Defining Limitation. The Board correctly found that it did, based on the substantial evidence of record. Notably, CPC does not and has never challenged the motivation to combine Hsu with any other reference in the grounds now on appeal or raised any secondary considerations.

Despite embracing the Board's construction of the Defining Limitation as "correct" (Blue Br. 11), CPC argues that the Board erred by re-interpreting or misapplying this limitation. According to CPC, the Board's application of its construction should have additionally required that the card information provide data that establishes the memory location or address at which the system will store the biometric signature. In CPC's view, the Board allegedly erred by mapping the claims to the mere "association" of card information and biometric signatures in a database to define a memory location. Though CPC's brief styles the issue on appeal as one of claim construction, CPC's argument raises only factual issues. The Board

correctly applied its construction of the Defining Limitation and found that Hsu's association of card information with biometric signatures in a database discloses the Defining Limitation. And this is supported by substantial evidence, including the disclosure of Hsu itself and the testimony of Petitioners' technical expert, Mr. Stuart J. Lipoff, explaining how one of ordinary skill in the art would have understood Hsu.

CPC also argues that the Board erred by "leap[ing]" to allegedly fill a gap in the prior art because, according to CPC, "Hsu is devoid of any disclosure that its ["card information"] includes data tethered to a specific database address." Blue Br. 23-24. But CPC's argument entirely ignores the role of one of ordinary skill in the art in its critique of the Board's analysis. Consistent with Federal Circuit precedent, the Board properly and correctly considered how one of ordinary skill in the art would have understood Hsu and did not limit itself to the express disclosures of the prior art. CPC's arguments to the contrary apply an incorrect and overly rigid standard for obviousness that has no legal support.

The Board's determination that claims 1-20 of the '039 patent are unpatentable for obviousness should be affirmed.

II. COUNTERSTATEMENT OF THE ISSUES

1. Whether substantial evidence supports the Board's finding that Hsu discloses the Defining Limitation, as properly construed and applied by the Board, where the Board found, citing Hsu's disclosure and the testimony of Petitioners'

technical expert, Mr. Lipoff, that Hsu teaches storing a biometric signature in a database in a memory location "associated with" a user's card information to expedite the process of matching a would-be user's biometric signature with reference biometric signatures.

III. COUNTERSTATEMENT OF THE CASE

A. The '039 Patent Claims Methods and Systems for Enrolling and Verifying Users in a Biometric Card Pointer System

The '039 patent describes methods and systems for enrolling a card (e.g., an ATM card or credit card) in a "Biometric Card Pointer" system and then verifying enrolled cards using that system. Appx273 at 2:51-61.

"[C]ard devices," such as credit cards or identification cards, contain "card information" that can be accessed using a "reader device." Appx273 at 1:21-32. To prevent an "unauthori[z]ed user" from using a card, mechanisms exist to verify the identity of the individual presenting the card, including requiring a biometric signature. Appx273 at 1:33-2:44. For example, a "card user swipes the standard card 701 through an associated card reader (not shown) that accesses the card information 702 on the card 701. The card user also provides a biometric input 801, for example[,] by pressing their thumb against a biometric ([e.g.,] fingerprint) reader 802." Appx273 at 2:10-22. Assuming the card owner "previously registered their biometric signature 801 and the card information 702 . . . onto [a] back-end database," a "back-end processor" compares the pre-loaded database information

with the received card information and fingerprint to "check that the card holder of the card 701 is the (authori[z]ed) card owner and that the card itself is valid, in which case the transaction in question can proceed." Appx273 at 2:23-31.

But, according to the '039 patent, "this arrangement requires a central repository (806) of card information 702 and biometric information 801," and results in a "cumbersome" process requiring "complex back-end database management." Appx273 at 2:31-39. These prior art systems required "search[ing] [an] entire database . . . to see if there is a [biometric] match." Appx276 at 8:37-38.

The '039 patent thus discloses a "Biometric Card Pointer" system to allegedly overcome the prior art's disadvantages. Appx273 at 2:51-64. As part of an enrollment process, when a card user uses a verification station for the first time, the Biometric Card Pointer system stores "a card user's biometric signature in a local memory in a verification station." *Id.* The system stores a user's biometric signature "at a memory address defined by the ('unique') card information on the user's card as read by the card reader of the verification station." Appx273 at 2:62-67. This concept is reflected in independent claim 1, including the disputed "Defining Limitation" emphasized below:

1. A method of enrolling in a biometric card pointer system,

the method comprising the steps of:

receiving card information;

receiving the biometric signature;

defining, dependent upon the received card information, a memory location in a local memory external to the card;

determining if the defined memory location is unoccupied; and

storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

Appx278 at 12:29-38 (emphasis added). When a card user later uses the enrolled card at the verification station, the Biometric Card Pointer system checks a newly scanned fingerprint "against the biometric signature" previously stored in the local memory at the "address defined by the card data 604." Appx276 at 8:5-37. This eliminates the "need to search the entire database 124 to see if there is a match." Appx276 at 8:34-41.

Independent claims 3, 13, 15, 18, and 19 recite variations of the Defining Limitation, and the remaining claims depend from one of these independent claims. Only the Defining Limitation is at issue in this appeal. Indeed, there is no dispute that independent claims 3, 13, 15, 18, and 19 include similar variations of the Defining Limitation for the purpose of this appeal.

B. Like the '039 Patent, Hsu Discloses Enrolling and Verifying Users in a Biometric Card Pointer System

Hsu teaches methods and systems "for controlling access to building doors or to machines, such as automatic teller machines (ATMs)," by verifying a user's identity using card information and a fingerprint. Appx943, Abstract; Appx944 ¶¶ 1,

6; Appx993 ¶¶ 32-33. Hsu discloses that, "[i]n the past, fingerprint matching systems have been relatively slow" because the "fingerprint matching system . . . must compare a sensed fingerprint image with many possible stored reference images" before verifying a would-be card user. Appx944 ¶ 4.

To overcome disadvantages in prior systems, Hsu teaches verifying a user by (1) "reading ***preliminary identification data*** supplied by a user seeking access"; (2) "sensing the user's fingerprint prior to granting access, and generating a fingerprint image"; (3) "***retrieving from a fingerprint database reference fingerprint data corresponding to the preliminary identification data***"; (4) "comparing the reference fingerprint data with the subject fingerprint image to verify the preliminary identification data and, if there is [a] match, generating a match signal"; and (5) "granting access to the secured building or machine if a match signal is generated." Appx944 ¶ 10 (emphases added).

To enable its verification method, Hsu discloses an "enrollment procedure" whereby its system initially stores a user's "reference fingerprint data" in a location corresponding to the user's preliminary identification data (e.g., "account number"). Appx946-947 ¶ 26. A user enrolls by presenting both "a finger to the fingerprint sensor 16, which generates a fingerprint image," and "an account number." *Id.* Hsu explains that "[t]he account number is stored in the database 44 in association with the user's fingerprint image data." *Id.* Hsu's Figure 4 illustrates its database storing

account numbers ("ACC. NOS.") and reference fingerprint images ("REF. PRINTS") in association with one another:

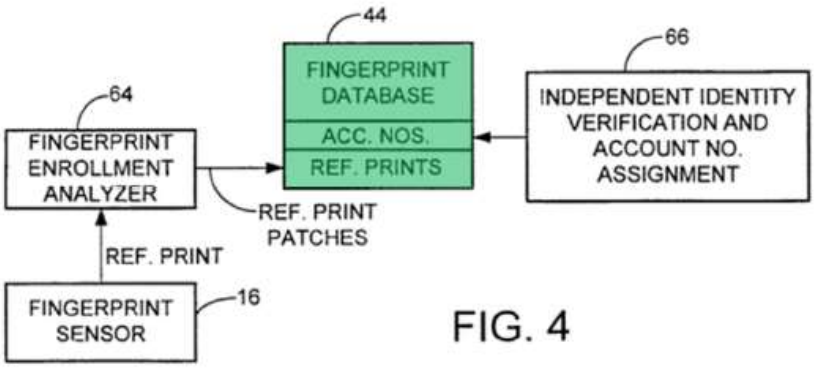

FIG. 4

Appx1024-1025 ¶ 93 (annotating Appx950 at Fig. 4).

Hsu discloses that a user's account number (or other "preliminary identification data") is also stored on a "machine readable card." Appx943, Abstract; Appx944 ¶ 7. Once enrolled, a user presents this card (including the account number), along with a fingerprint, to a system that then verifies that the user's fingerprint matches a stored fingerprint image associated with the account number. Appx945-946 ¶¶ 13, 20. Hsu explains that storing a user's reference fingerprint image in a location "associated with" a user's account number allows "fingerprint matching" to "be achieved rapidly," eliminating the need to "compare a sensed fingerprint with many possible stored reference images." Appx944-945 ¶¶ 13, 4.

C. The Board Found All Challenged Claims Unpatentable as Obvious over Hsu in Combination with Various Secondary References

Petitioners filed two petitions (IPR2022-01093 and IPR2022-01094), including eight total grounds, together challenging all 20 claims of the '039 patent. Appx282-388; Appx389-496. In support of both petitions, Petitioners cited the testimony of technical expert, Mr. Lipoff. Appx976-1185; Appx3139-3175.

The Board determined that Petitioners prevailed against every challenged claim. Appx1-58; Appx59-125. In IPR2022-01093, the Board found challenged claims 1, 2, 13, 14, 19, and 20 unpatentable under Ground 1, and therefore did not reach the additional arguments as to those claims in Ground 2. Appx56 n.11. In IPR2022-01094, the Board found challenged claims 3-12 and 15-18 unpatentable under Grounds 1, 3, 5, and 7, and therefore did not reach the additional arguments as to those claims in Grounds 2, 4, 6, and 8. Appx123-124 nn.17-20. In making these determinations, the Board found that Hsu discloses the Defining Limitation as recited in some form in each independent claim. *See* Appx32-39; Appx91-98. The Board's findings relied on Hsu's disclosure and on testimony from Mr. Lipoff describing how one of ordinary skill in the art would understand Hsu's disclosure. *See* Appx32-39; Appx91-98.

1. The Board Construed "Dependent Upon" and "Defining, Dependent Upon the Received Card Information, a Memory Location in a Local Memory External to the Card"

The Board construed two relevant claim terms, neither of which CPC disputes on appeal. First, the Board construed "dependent upon" (claims 1 and 19) to have its plain and ordinary meaning: "contingent upon or determined by." Appx14; Appx75.

Second, the Board construed "defining, dependent upon the received card information, a memory location in a local memory external to the card," finding that "defining, dependent upon . . ." means that "during an enrollment process[,] the claimed 'biometric signature,' e.g., a fingerprint, is not yet stored in the memory, and no memory location or address has been 'defined,' as in 'set' or 'established,' in the memory for storing the fingerprint, until card information is received." Appx16. CPC does not dispute either of these constructions on appeal.

2. The Board Found that Hsu Discloses the Defining Limitation

CPC made a single argument regarding the prior art across both proceedings: that Hsu does not disclose the Defining Limitation. Appx39; Appx43-45; Appx97-99; Appx102; Appx103; Appx109; Appx110; Appx112. CPC did not below and does not now challenge the motivation to combine Hsu with any other reference in the grounds now on appeal or raise any secondary considerations. The Board

disagreed with CPC's argument and found, based on Hsu's disclosure and Mr. Lipoff's testimony, that Hsu discloses the Defining Limitation.

First, the Board found that "Hsu tells us a location, that is[,] *where*, i.e., in fingerprint database 44, the fingerprint is to be stored during enrollment." Appx33. The Board found: "Hsu explains that in fingerprint database 44, 'fingerprint data are associated with corresponding user numbers . . . .'" Appx33 (quoting Appx946-947 ¶ 26). Thus, the Board concluded "that the user's fingerprint is stored in relation to, i.e., 'associated with,' the user's employee account number, for example." Appx33 (quoting Appx946-947 ¶ 26). The Board grounded its finding in expert testimony, explaining that "Mr. Lipoff testifies persuasively that in Hsu[,] '[t]he "fingerprint image . . ." [is] not stored at *any* memory location in the database—rather, it is stored at a memory location associated with the specific user/employee number received from a card.'" Appx34-35 (second alteration in original) (quoting Appx1024-1025 ¶ 93).

Second, the Board found that Hsu disclosed "*how* . . . the fingerprint data [is] stored during enrollment." Appx33. The Board explained that Hsu's "card information must 'set' or 'establish' where the fingerprint data is to be stored" for Hsu to disclose the Defining Limitation. Appx33. According to the Board, "Hsu explains that when a user presents a fingerprint during enrollment, '[a]t the same time, the user's identity has to be independently verified, by some means other than

fingerprint matching, . . . and the user also presents an account number, employee number[,] or similar identity number.'" Appx33 (first alteration in original) (quoting Appx946-947 ¶ 26). Thus, the Board concluded, "during enrollment[,] Hsu stores the user's fingerprint data 'associated with' a user's employee number on the card" such that "the identification information, e.g., employee number, on the identification card defines, sets, or establishes *where* the fingerprint is stored; that is, the user's fingerprint data is stored with the database record corresponding to the relevant employee number." Appx33-34 (citing Appx944-945 ¶ 11).

The Board again "credit[ed] Mr. Lipoff's testimony that even though Hsu does not explain exactly 'how a new user record is created' during enrollment, a person of ordinary skill in the art would 'try using simple known options for creating database records.'" Appx36-37 (quoting Appx3160-3161 ¶¶ 33). The Board continued: "Mr. Lipoff explains persuasively that 'upon a user enrolling, they provide a previously unseen card/user number, [and] the system then creates a new record for the user, including setting/establishing for the first time the memory location for storing the user's fingerprint.'" Appx36-37 (alteration in original) (quoting Appx3161 ¶ 34). The Board noted that Mr. Lipoff explained "that it is the user's employee or account number that defines where the fingerprint data is stored[.]" Appx37-38 (citing Appx2948-2949 at 33:16-34:9).

The Board rejected each of CPC's arguments regarding the Defining Limitation. The Board noted that CPC's "argument mainly contrasts the terms 'associated with,' as described in Hsu, with our claim construction that 'defined by,' means 'set' or 'established.'" Appx34. The Board "agree[d] that these are different words," but it found that "an ordinary meaning of 'associated' is 'related, connected, or combined together.'" Appx34 (quoting Appx3712). Rejecting CPC's argument, the Board found that, "[c]onsidering common database structures and functions, we are persuaded that Hsu, by 'associating' a user's fingerprint data with a database record corresponding to a particular employee, concomitantly discloses 'defining,' 'setting,' or 'establishing' a memory location for the fingerprint data in relation to the employee account number." Appx34.

IV. SUMMARY OF THE ARGUMENT

The Court should affirm the Board's Final Written Decisions, which determined that claims 1-20 of the '039 patent are unpatentable as obvious. First, substantial evidence supports the Board's finding that Hsu discloses the Defining Limitation by disclosing storing a biometric signature (a fingerprint image) in a memory location defined by card information by requiring that the fingerprint image be stored in a location "associated with" the user's card information. The issue is one of substantial evidence—not claim construction as CPC contends. CPC contrasts the dictionary definitions of the terms "associated with" (as used by Hsu) and the

terms "defined," "set," and "established" (as used in the Board's claim construction). But the Board embraced that "associated with" is a different word than "defined," "set," or "established." Rather than equating the *meaning* of the term "associated" with "define," "set," or "establish," the Board found that it is the *effect* of Hsu's association that results in its disclosure of the claimed feature. This finding was supported by the testimony of Petitioners' technical expert, Mr. Lipoff.

Second, contrary to CPC's arguments, the Board neither made findings based on its own experience nor made any improper "leap" in evaluating Hsu's disclosure. CPC contends that Hsu does not disclose "that its employee number includes data tethered to a specific database address" and the Board made a "leap" to "connect the necessary dots to conclude that Hsu discloses the Defining Limitation." Blue Br. 23-24. But the Board properly credited Mr. Lipoff's testimony explaining that one of ordinary skill in the art would have understood that the user number defines the memory location in which the stored fingerprint image will be stored because Hsu's database structure is one that starts with the user number telling you where to find the memory location that has the stored fingerprint image. CPC's arguments rely on an incorrect obviousness framework that fails to consider how one of ordinary skill in the art would read the prior art.

V. ARGUMENT

A. Standard of Review

Obviousness is a question of law based on underlying factual findings. *See In re Baxter Int'l, Inc.*, 678 F.3d 1357, 1361 (Fed. Cir. 2012). The Federal Circuit reviews the legal question de novo but the underlying factual determinations (such as "the determination of what a reference teaches" or how one of ordinary skill would have understood a reference) for substantial evidence. *Id*.

Substantial evidence exists where "a reasonable mind might accept the evidence to support the finding." *Id.*; *In re Gartside*, 203 F.3d 1305, 1312 (Fed. Cir. 2000); *see Consol. Edison Co. v. NLRB*, 305 U.S. 197, 229-30 (1938). "[W]here two different, inconsistent conclusions may reasonably be drawn from the evidence in record, an agency's decision to favor one conclusion over the other is the epitome of a decision that must be sustained upon review for substantial evidence." *In re Jolley*, 308 F.3d 1317, 1328-29 (Fed. Cir. 2002).

The Federal Circuit also "defer[s] to the Board's findings concerning the credibility of expert witnesses." *Yorkey v. Diab*, 601 F.3d 1279, 1284 (Fed. Cir. 2010) (citation omitted).

B. The Board Correctly Applied Its Construction of "Defining, Dependent Upon the Received Card Information, a Memory Location in a Local Memory External to the Card" to Hsu

Despite CPC's attempt to characterize the issues on appeal as legal in nature, CPC ultimately disputes the Board's factual finding that Hsu discloses the Defining

Limitation, including both the scope of Hsu's disclosure and how one of ordinary skill in the art would have understood Hsu. But the Board's findings are supported by substantial evidence, and, in analyzing Hsu, the Board did not broaden or otherwise alter the scope of its construction of the Defining Limitation.

1. Substantial Evidence Supports the Board's Finding that Hsu Discloses or Suggests the Defining Limitation

In determining that Hsu discloses the Defining Limitation, the Board found that Hsu described both *where* a biometric signature is stored and *how* it is stored. Appx33-39. Substantial evidence, in the form of both Hsu's disclosure and Mr. Lipoff's testimony, supports the Board's findings.

The Board first found that Hsu discloses "*where*, i.e., in fingerprint database 44, the fingerprint is to be stored during enrollment." Appx33. The Board found that Hsu's card information (e.g., an "employee number") "defines, sets, or establishes" the location in fingerprint database 44 where the fingerprint data is stored. Appx33-34. The Board anchored its decision in Hsu and Mr. Lipoff's testimony.

As the Board found, Hsu's "fingerprint database 44 contains reference fingerprint image data for each user, employee, or customer using the system." Appx32-33 (quoting Appx946-947 ¶ 26). Hsu discloses that its "fingerprint database 44" "is basically a table that associates each user number with a stored fingerprint image," and that the database "may also contain other information about

the user." Appx945-946 ¶ 20. Thus, according to the Board, Hsu discloses storing fingerprint data ("biometric signature") in a location that is "relat[ed] to, i.e., 'associated with,' the user's employee account number, for example." Appx33 (quoting Appx946-947 ¶ 26).

Hsu's Figure 4 illustrates the "location, that is[,] *where*, i.e., in fingerprint database 44, the fingerprint is to be stored during enrollment":

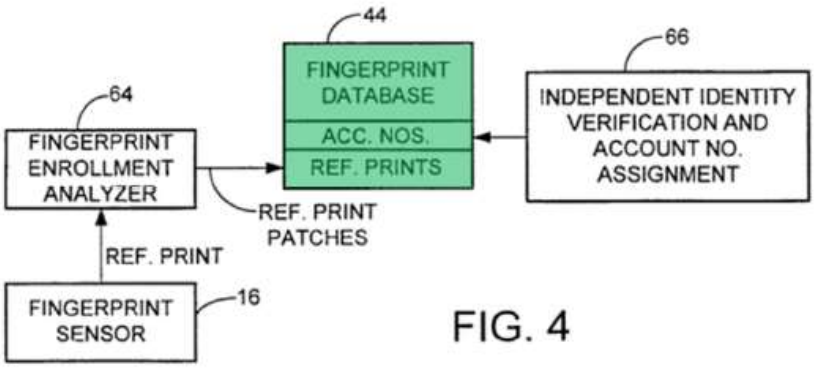

FIG. 4

Appx32-33 (reproducing the annotation of Appx950 at Fig. 4 from Appx1024-1025 ¶ 93). Figure 4 shows that Hsu discloses storing a user's reference fingerprint data ("REF. PRINTS") under that user's account number ("ACC. NOS."). Appx1024-1025 ¶ 93; Appx950 at Fig. 4.

The Board correctly credited Mr. Lipoff's testimony that one of ordinary skill would have understood that in Hsu, "[t]he 'fingerprint image, or [] selected distinctive attributes or features of the user's fingerprint image' are not stored at ***any*** memory location in the database—rather, it is stored at a memory location associated

with the specific user/employee number received from a card." Appx34-35 (alterations in original) (emphasis added) (quoting Appx1024-1025 ¶ 93).

The Board also found that Hsu discloses not only *where* but also *how* fingerprint data is stored during enrollment—by "receiv[ing] data indicative of, for instance, an employee number from a user's identification badge [(i.e., "card information")], which thus defines a database record with which the fingerprint data can be 'associated.'" Appx36. Again, this finding is also supported by substantial evidence, including Hsu and Mr. Lipoff's testimony.

Hsu's "enrollment procedure requires that each user enroll by presenting a finger to the fingerprint sensor 16, which generates a fingerprint image for a fingerprint enrollment analyzer 64." Appx946-947 ¶ 26. "At the same time, the user's identity has to be independently verified, by some means other than fingerprint matching, as indicated in block 66, and the user also presents an account number, employee number[,] or similar identity number." *Id.* From this, the Board correctly found that "Hsu describes presenting identification data apart from biometric data, and includes presenting, for example, an employee identification card or badge, including the user's employee number." Appx33-34 (citing Appx944-945 ¶ 11).

Hsu further discloses that during enrollment, after collecting a fingerprint image and account number, "[t]he account number is stored in the database 44 in

association with the user's fingerprint image data." Appx946-947 ¶ 26. The Board thus correctly found that, since "during enrollment[,] Hsu stores the user's fingerprint data" in a location "'associated with' a user's employee number," and "the identification information, e.g., employee number[] on the identification card[,] defines, sets, or establishes *where* the fingerprint is stored; that is, the user's fingerprint data is stored with the database record corresponding to the relevant employee number." Appx34.

The Board also relied on Mr. Lipoff's testimony that one of ordinary skill would have been aware of "simple known options for creating database records." Appx36-37 (quoting Appx3160-3161 ¶ 33). For example, Mr. Lipoff explained, one of ordinary skill would have known "to create a new user record upon enrollment." Appx3161 ¶ 34 (citing Appx946-947 ¶ 26). Mr. Lipoff testified that "upon a user enrolling, they provide a previously unseen card/user number, [and] the system then creates a new record for the user, including setting/establishing for the first time the memory location for storing the user's fingerprint." Appx37 (alteration in original) (quoting Appx3161 ¶ 34). The Board relied on Mr. Lipoff's description of "Hsu's database structure and functions" when he testified that Hsu's "database is basically a table that associates each user number with a stored fingerprint image or selected attributes." Appx37-38 (citing Appx2948-2949 at 33:16-34:9). Mr. Lipoff explained that "the user number is defining the memory location in which the stored fingerprint

image will be stored because the structure of the database is one . . . that starts with the user number telling you where to find the memory location that has the stored fingerprint image." *Id.*

2. The Board Did Not Broaden Its Construction of the Defining Limitation

Contrary to CPC's arguments, the Board did not alter its construction of the Defining Limitation. *See In re Aspen Aerogels, Inc.*, 835 F. App'x 587, 589 (Fed. Cir. 2020) (rejecting characterization of argument as a legal question and instead finding, where "[t]here is no formal construction of the term . . . that [appellant] disputes," that "the issue [is] a factual question").

CPC contends that, aside from the dictionary definition of "associated," "the Board cited no further basis for the conclusion that 'defining' also means or includes 'associated with.'" Blue Br. 17. But the Board referenced a dictionary definition of the word "associated," not in support of its own decision, but to refute CPC's argument that "mainly contrasts the terms 'associated with,' as described in Hsu, with [the Board's] claim construction that 'defined by[]' means 'set' or 'established.'" Appx34. At no point did the Board suggest "that 'defining' also means or includes 'associated with.'" Blue Br. 17. To the contrary, the Board embraced that "these are different words." Appx34.

Far from equating the *meaning* of the term "associated" with "define[]," "set," or "establish[]," the Board found that it is the *effect* of Hsu's association that results

in its disclosure of the claimed feature. Appx34-35. The Board found that Hsu's disclosure of associating fingerprint data with user or account numbers in a database meets the claimed requirement that card information provides data that establishes where, i.e., at what memory location or address, the system will store the fingerprint data. Appx33-34. This is supported by Hsu (*e.g.*, Appx946-947 ¶ 26) and Mr. Lipoff (*e.g.*, Appx1024-1025 ¶ 93; Appx3160-3161 ¶¶ 33-34; Appx2948-2949 at 33:16-34:12). This is also supported by CPC's characterization of the challenged claims during oral argument: "All we're saying that Claim 1 requires is that when a user swipes their card, that is the information that is on the card, not -- in that moment in time, not something else in the system, but the information on the card that directs the system where to store that particular user's fingerprint or other biometric data." Appx3678 at 31:7-11; *see* Appx16 (citing same).

CPC's arguments rely on an incorrect framework for analyzing the prior art in view of the claim language. CPC contends that (1) "Petitioner[s] never proposed a construction of 'defining' that includes 'in association with'" (Blue Br. 20 n.7 (citation omitted)); and (2) "[t]he Board cited neither the specification nor the file history for any intrinsic evidence that 'defining' as used in the '039 Patent claims includes mere 'association'" (Blue Br. 17). But CPC provides no basis for its argument that the Board, in evaluating whether Hsu's disclosure meets the claim language (as construed), was required to find the exact words of its construction in

the prior art or in the intrinsic evidence. Indeed, as the Federal Circuit has explained, "'[t]he invention is not the language of the [claim] but the subject matter thereby defined.' . . . Thus, a prior art inventor need not 'conceive of its invention using the same words as the patentee would later use to claim it.'" *Adasa Inc. v. Avery Dennison Corp.*, 55 F.4th 900, 913 (Fed. Cir. 2022) (second alteration in original) (citations omitted), *cert. denied*, 143 S. Ct. 2561 (2023).

CPC's argument "misapprehends the obviousness inquiry, which is not limited to the express disclosures of the prior art but instead involves what 'a person of ordinary creativity . . .' would understand from the prior art." *GUI Glob. Prods., Ltd. v. Samsung Elecs. Co.*, No. 2022-2156, -2157, -2158, -2159, 2024 WL 1564694, at *3 (Fed. Cir. Apr. 11, 2024) (quoting *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007)). And this is how the Board, correctly, conducted its inquiry. Guided by Mr. Lipoff's testimony, the Board found that "defining . . . a memory location," as claimed, is met by Hsu's disclosures of storing an "account number . . . in the database 44 in association with the user's fingerprint image data." Appx32-39 (citations omitted).

CPC contends that "[j]ust because two items are 'related, connected[,] or combined together' in storage does not logically mean that one of the items is the item that provides the data that 'sets' or 'establishes' the particular address at which

the other item will be stored."[3] Blue Br. 18. But the Board correctly found that, in the context of Hsu's database (and databases more generally), when two items are connected (i.e., associated), the first item (e.g., card information) does "set" or "establish" the location of the second item (e.g., the fingerprint data). And that is true based on the nature of the relationship between the data and its storage, despite the absence of the specific words "defined," "set," or "established" in Hsu. Appx2948-2949 at 33:16-34:12. As Mr. Lipoff testified, "[t]he account number is the item that's used to indicate the location where the fingerprint image is going to be stored and to be subsequently accessed." Appx2947-2949 at 32:19-34:9.

Indeed, Hsu teaches that the "preliminary identification data" (e.g., "account number") is the primary piece of data for a particular user with which all other user data is associated. For example, Hsu teaches that a "user number" acts as a reference point for a particular database location because Hsu discloses that its database

[3] According to CPC, "[m]ore is needed" (Blue Br. 18), yet CPC's arguments fail to make clear what "[m]ore" is required from "define," "set," or "establish." During oral argument, the Administrative Patent Judge asked whether the "information on the card" needed to be, "in of itself, the blocker bit physical location in memory." Appx3687-3688 at 40:23-41:9. CPC declined to agree, instead arguing that "it's the data on the card that sets or establishes the location in memory, where the biometric signature will be stored." Appx3689 at 42:1-3. CPC's counsel further argued that, "in Hsu, there is no card information that dictates where in memory, during enrollment, the fingerprint will be stored." Appx3689 at 42:3-5. But this is contrary to the substantial evidence discussed in Section V.B.1.

contains "a stored fingerprint image" corresponding to that user number and additional "information about the user, such as a history of access to the door." Appx945-946 ¶ 20. Notably, Hsu does not say that this "information about the user" is associated with a stored fingerprint image—the information is associated with the "user number." *Id.* Thus, the Board correctly concluded that Hsu's card information "sets" or "establishes" the memory location for the biometric signature.

The '039 patent is consistent with the Board's application of the construed claim language to Hsu. The '039 patent discloses that "[t]he biometric signature is stored at a memory address defined by the ('unique') card information on the user's card as read by the card reader of the verification station." Appx273 at 2:64-67. During an "enrol[l]ment phase," "[t]he card data 604 defines the location 607 in the memory 124 where [the] unique biometric signature is stored." Appx276 at 7:43-49. And during the verification phase, just like in Hsu, "the card data 604 acts as the memory reference which points . . . to a particular memory location at an address 607 in the local database 124." Appx276 at 7:31-35. According to the '039 patent, this is shown in Figure 4. Appx269 at Fig. 4; Appx276 at 7:24-42. These disclosures are consistent with the Board's finding that Hsu discloses storing fingerprint data at a location defined by the biometric signature.

CPC's analogy to the facts of *In re Abbott Diabetes Care Inc.*, 696 F.3d 1142 (Fed. Cir. 2012), to create a claim construction argument is inapposite. *See* Blue Br.

20. In that case, the Board construed "substantially fixed" to mean "allow[ing] some movement." *In re Abbott*, 696 F.3d at 1147, 1150-51 (alteration in original). But, according to the Federal Circuit, the Board acted unreasonably when it equated "allow[ing] some movement" to "somewhat restrained in movement." *Id.* (alteration in original). The Federal Circuit thus remanded for the Board to apply its original construction. *Id.* at 1151. Unlike that appeal, here substantial evidence supports the Board's finding that "defining," which was construed to mean "set" or "establish," is met by Hsu's disclosure of associating one set of data with another set of data. This is "defining . . . a memory location" and not some modification of the Board's claim construction.

Similarly, *D'Agostino v. MasterCard International Inc.*, 844 F.3d 945, 950 (Fed. Cir. 2016), does not show that CPC raises a claim construction dispute. Blue Br. 20-21 (citing *D'Agostino*, 844 F.3d at 950). In that case, a claim element required that a patent request be limited to "a single merchant," which was construed to mean that "the request limits the number of authorized merchants to one but does not then identify the merchant[.]" *D'Agostino*, 844 F.3d at 947-48, 950. The Federal Circuit found that the Board "departed from or misapplied" the proper construction by finding that a "chain of stores" can be a "single merchant." *Id.* at 950 (citation omitted). The Federal Circuit found that the Board's application of its construction contradicted the "straightforward logic" of the claim, as well as the prosecution

history. *Id.* at 949-50. In this case, however, the Board's application of its construction to Hsu is consistent with the intrinsic evidence and is supported by substantial evidence within Hsu itself and Mr. Lipoff's testimony.

C. Appellant's Remaining Arguments Do Not Undermine the Substantial Evidence Supporting the Board's Finding that Hsu Discloses the Defining Limitation

CPC contends that Hsu does not disclose "that its employee number includes data tethered to a specific database address," and the Board made a "leap" to "connect the necessary dots to conclude that Hsu discloses the Defining Limitation." Blue Br. 23-24. CPC contends a "leap" was necessary because "there is no disclosure in Hsu that the 'user's personal data record' has any relationship to any specific memory location." Blue Br. 24. But the Board found that the user number defines the memory location via Hsu's database 44. *See* Appx32-35. And the Board's finding is supported by substantial evidence, including Mr. Lipoff's testimony. *See supra* Section V.B.1. Mr. Lipoff explained that "the user number is defining the memory location in which the stored fingerprint image will be stored because the structure of the database is one . . . that starts with the user number telling you where to find the memory location that has the stored fingerprint image." Appx2948-2949 at 33:16-34:12.

Citing *In re Zurko*, 258 F.3d 1379 (Fed. Cir. 2001), CPC contends that "the Board cannot simply reach conclusions based on its own understanding or

experience -- or on its assessment of what would be basic knowledge or common sense. Rather, the Board must point to some concrete evidence in the record in support of these findings." Blue Br. 17-18 n.6, 26-27 n.10 (quoting *In re Zurko*, 258 F.3d at 1386). But the Board relied on Mr. Lipoff's testimony (*see supra* Section V.B.1), and CPC's argument that the Board reached its findings on its own has no basis in the record.

CPC's contention that the Board based its decision on "'common database structures and functions' that the Board did not identify" (Blue Br. 17-18) is mistaken. *Directly* after the Board referenced "common database structures and functions," it cited Mr. Lipoff's testimony describing those structures and functions. Appx34-35 (citing Appx946-947 ¶ 26; Appx1024-1025 ¶ 93). The Board identified Hsu's depiction of "database structure[s] and functions" in Hsu's Figure 4 and highlighted Hsu's description of its database as "a table that associates each user number with a stored fingerprint image." Appx37-38 (quoting Appx2948-2949 at 33:16-34:9) (citing Appx2949-2950 at 34:19-35:9); *see also* Appx945-946 ¶ 20; Appx946-947 ¶ 26; Appx950 at Fig. 4. The Board further cited Mr. Lipoff's explanation that Hsu's fingerprint image is "not stored at *any* memory location in the database—rather, it is stored at a memory location associated with the specific user/employee number received from a card." Appx34-35 (quoting Appx1024-1025

¶ 93) (citing Appx946-947 ¶ 26); *see also* Appx37-38 (citing Appx2948-2949 at 33:16-34:9); Appx38 (citing Appx2949-2950 at 34:19-35:9).[4]

CPC applies an incorrect and overly rigid standard for obviousness, which fails to account for the perspective of one of ordinary skill in the art. The Federal Circuit has expressly rejected CPC's obviousness framework, finding that the Board errs when it adopts a "rigid approach to determining obviousness based on the disclosures of individual prior-art references, with little recourse to the knowledge, creativity, and common sense that an ordinarily skilled artisan would have brought to bear." *Randall Mfg. v. Rea*, 733 F.3d 1355, 1362 (Fed. Cir. 2013).

CPC's criticism of Mr. Lipoff's testimony is also unavailing. *See* Blue Br. 26-27. The Board made a credibility determination with which CPC disagrees: the Board found that Mr. Lipoff "testifies persuasively" (Appx34-35) and "explains persuasively" (Appx37), leading the Board to "credit" his testimony regarding Hsu's

[4] Contrary to CPC's arguments (Blue Br. 17-18 n.6, 26-27 n.10), the Board did not resort to common-sense reasoning to supply a missing claim limitation. Regardless, CPC fails to demonstrate that such reasoning would have been improper given the Board's thorough analysis and the expert's testimony. *See B/E Aerospace, Inc. v. C&D Zodiac, Inc*, 962 F.3d 1373, 1380 (Fed. Cir. 2020) (affirming the Board's invocation of common sense where "[t]he Board dedicated more than eight pages of analysis to the [claim] limitation and relied on [a technical expert's] detailed expert testimony"); *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1361 (Fed. Cir. 2016) (recognizing that common sense and common knowledge can, under certain circumstances, even be used to supply a missing limitation).

disclosure (Appx36-37). Mr. Lipoff tethered his testimony to the prior art and explained how one of ordinary skill would have understood Hsu's disclosure. *See supra* Section V.B.1. CPC provides no basis to challenge that finding on appeal. *See ESIP Series 2, LLC v. Puzhen Life USA, LLC*, 958 F.3d 1378, 1384 (Fed. Cir. 2020) ("We find no error in the Board's decision to credit the opinion of one expert over another, and we do not reweigh evidence on appeal." (citation omitted)).

CPC contends, without any supporting authority, that Mr. Lipoff must cite "independent or corroborative evidence, such as prior art publications or products." Blue Br. 26. But Mr. Lipoff *did* cite corroborative evidence, including Hsu itself and CPC's own expert (via the Patent Owner's Response). Appx3161 ¶ 34 (citing Appx946-947 ¶ 26; Appx3123 at 107:15-19; Appx3124 at 111:8-12; Appx2789); *see also* Appx2789 (citing Appx2894-2895 ¶ 67)). And, even if Mr. Lipoff had not cited corroborative evidence, he can still testify based on his own experience. *See* Fed. R. Evid. 702(a) ("[T]he expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence . . . ."); *see also* 37 C.F.R. § 42.62(a) ("[T]he Federal Rules of Evidence shall apply to a proceeding.").

CPC contends that the Board's finding that Hsu explains how the account number and fingerprint data are stored in the fingerprint database "is contrary to Petitioner[s'] own admission that '*Hsu is silent on how a new user record is created*'

during enrollment." Blue Br. 27 (quoting Appx3160-3161 ¶ 33). But the Board correctly rejected the suggestion that "'defining . . . a memory location,' or Patent Owner's alternative wording, 'establishing' or 'setting,' means '[*creating*] . . . a memory location in a local memory.'" Appx15 (alteration in original) (quoting *Apple, Inc. v. CPC Pat. Techs. PTY, Ltd*, IPR2022-00600, Paper 22 at 32 (PTAB Oct. 13, 2023)). CPC does not challenge this aspect of the Board's construction on appeal. Thus, under the Board's unchallenged construction, Hsu need not explain "how a new user record is created" to disclose the Defining Limitation; it need only disclose that the received card information sets or establishes the memory location for the biometric signature, as discussed above.

But regardless of whether Hsu is silent on the issue, the Board properly cited and relied upon Mr. Lipoff's explanation that, given Hsu's disclosure and an ordinary artisan's knowledge of databases, "it would have been obvious for a POSITA to try using simple known options for creating database records." Appx36-37 (citing Appx3160-3161 ¶ 33). And Mr. Lipoff provided a concrete example, explaining that "[o]ne option is to store all the user numbers in Hsu's database and reserve/pre-establish memory locations for associated fingerprint data. Upon a user enrolling by providing a user number, the system looks up the user number and determines the corresponding memory location for storing the user's fingerprint." Appx36-37 (citing Appx3160-3161 ¶ 33).

VI. CONCLUSION

For these reasons, this Court should affirm the Board's Final Written Decisions that claims 1-20 of the '039 patent are unpatentable for obviousness.[5]

[5] If the Court were to reverse on the two unpatentability grounds addressed by the Board (e.g., Ground 1 from IPR2022-01093 and Grounds 1, 3, 5, and 7 from IPR2022-01094), the Court should remand for further consideration of Ground 2 from IPR2022-01093 and Grounds 2, 4, 6, and 8 from the IPR2022-01094, which the Board declined to reach in the Final Written Decisions (Appx56 n.11; Appx123-124 nn.17-20).

Date: August 7, 2024

Respectfully submitted,

/s/Lionel M. Lavenue

Lionel M. Lavenue
Finnegan, Henderson, Farabow,
Garrett & Dunner, LLP
1875 Explorer Street, 8th Floor
Reston, VA 20190
(571) 203-2700

Kara A. Specht
Benjamin A. Saidman
Finnegan, Henderson, Farabow,
Garrett & Dunner, LLP
271 17th Street NW, Suite 1400
Atlanta, GA 30363
(404) 653-6400

Jonathan J. Fagan
Finnegan, Henderson, Farabow,
Garrett & Dunner, LLP
901 New York Avenue, NW
Washington, DC 20001-4413
(202) 408-4000

Attorneys for Appellees ASSA ABLOY AB, ASSA ABLOY Inc., HID Global Corp., ASSA ABLOY Global Solutions, Inc., and Master Lock Company, LLC

CERTIFICATE OF COMPLIANCE

The foregoing brief complies with the relevant type-volume limitation of the Federal Rules of Appellate Procedure and Federal Circuit Rules because:

> The brief has been prepared using a proportionally spaced typeface and includes 7,504 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f) and Fed. Cir. R. 32(b)

Date: August 7, 2024

/s/ Lionel M. Lavenue
Lionel M. Lavenue